e) die Verschlüsselung von Netzwerkverbindungen über Unternehmensnetzwerke, öffentliche Netzwerke, inländische Netzwerke, Netzwerke Dritter und drahtlose Netzwerke für die verwendeten Kommunikationsprotokolle unter Berücksichtigung der Ergebnisse der genehmigten Datenklassifizierung, der Ergebnisse der IKT-Risikobewertung und der Verschlüsselung von Netzwerkverbindungen gemäß Artikel 6 Absatz 2;

f) die Konzeption der Netzwerke im Einklang mit den vom Finanzunternehmen festgelegten IKT-Sicherheitsanforderungen unter Berücksichtigung führender Praktiken zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks;

g) die Sicherung des Netzwerkverkehrs zwischen den internen Netzwerken und dem Internet und anderen externen Verbindungen;

h) die Ermittlung der Aufgaben und Verantwortlichkeiten sowie der Etappen für die Spezifikation, Implementierung, Genehmigung, Änderung und Überprüfung der Firewall-Regeln und Verbindungsfilter;

i) die Überprüfung der Netzwerkarchitektur und des Konzepts für die Netzwerksicherheit einmal jährlich und für Kleinstunternehmen in regelmäßigen Abständen, um potenzielle Schwachstellen zu ermitteln;

j) die Maßnahmen zur vorübergehenden Isolierung von Teilnetzwerken sowie von Netzwerkkomponenten und -geräten, soweit erforderlich;

k) die Implementierung einer sicheren Konfigurationsbasis für alle Netzwerkkomponenten und die Absicherung des Netzwerks und der Netzwerkgeräte im Einklang mit etwaigen Anweisungen des Anbieters und gegebenenfalls mit Normen im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 sowie führenden Praktiken;

l) die Verfahren zur Begrenzung, Sperrung und Beendigung von System- und Fernsitzungen nach einer bestimmten Inaktivitätszeit;

m) für Vereinbarungen über Netzwerkdienstleistungen:

   i) die Ermittlung und Spezifikation von IKT- und Informationssicherheitsmaßnahmen, der Dienstleistungsgüte und von Managementanforderungen für alle Netzwerkdienste;

   ii) die Feststellung, ob diese Dienstleistungen von einem gruppeninternen IKT-Dienstleister oder von IKT-Drittdienstleistern erbracht werden.

Für die Zwecke von Buchstabe h überprüfen die Finanzunternehmen regelmäßig die Firewall-Regeln und die Verbindungsfilter im Einklang mit der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 festgelegten Klassifizierung und dem Gesamtrisikoprofil der beteiligten IKT-Systeme. Bei IKT-Systemen, die kritische oder wichtige Funktionen unterstützen, überprüfen Finanzunternehmen mindestens alle sechs Monate, ob die bestehenden Firewall-Regeln und Verbindungsfilter angemessen sind.

Artikel 14

Sicherung von Informationen bei der Übermittlung

(1) Die Finanzunternehmen entwickeln, dokumentieren und implementieren im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten Richtlinien, Verfahren, Protokolle und Tools zum Schutz von Informationen, die übermittelt werden. Die Finanzunternehmen gewährleisten insbesondere Folgendes:

a) die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten während der Übermittlung über das Netzwerk und die Festlegung von Verfahren, um zu bewerten, ob diese Anforderungen eingehalten werden;

b) die Verhinderung und Erkennung von Datenlecks und die sichere Übertragung von Informationen zwischen dem Finanzunternehmen und externen Parteien;

c) die Implementierung, Dokumentation und regelmäßige Überprüfung der Anforderungen an Vertraulichkeits- oder Geheimhaltungsvereinbarungen, die dem Bedarf des Finanzunternehmens hinsichtlich des Schutzes von Informationen im Zusammenhang mit den Mitarbeitern des Finanzunternehmens und Dritten Rechnung tragen.

(2) Die Finanzunternehmen konzipieren die Richtlinien, Protokolle und Tools zum Schutz von Informationen bei der Übermittlung nach Absatz 1 auf der Grundlage der Ergebnisse einer genehmigten Datenklassifizierung und der IKT-Risikobewertung.

ABSCHNITT 7

IKT-Projekt- und -Änderungsmanagement

Artikel 15

IKT-Projektmanagement

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien für das IKT-Projektmanagement.

(2) In den in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement werden die Elemente festgelegt, die ein wirksames Management der IKT-Projekte in Bezug auf die Beschaffung, die Wartung sowie gegebenenfalls die Entwicklung der IKT-Systeme des Finanzunternehmens gewährleisten.

(3) Die in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement müssen alles Folgende beinhalten:

a) die Ziele des IKT-Projekts,

b) die Governance des IKT-Projekts, samt Aufgaben und Zuständigkeiten,

c) die Planung, den zeitlichen Rahmen und die Etappen des IKT-Projekts,

d) eine IKT-Projektrisikobewertung,

e) die relevanten Etappenziele,

f) die Anforderungen an das Änderungsmanagement,

g) das Testen aller Anforderungen, einschließlich der Sicherheitsanforderungen, und das zugehörige Genehmigungsverfahren bei der Einführung eines IKT-Systems in der Produktionsumgebung.

(4) Durch Bereitstellung der erforderlichen Informationen und Fachkenntnisse aus dem Geschäftsbereich oder den geschäftlichen Funktionen, auf die sich das IKT-Projekt auswirkt, gewährleisten die in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement die sichere Durchführung des Projekts.

(5) Der in Absatz 3 Buchstabe d genannten IKT-Projektrisikobewertung entsprechend müssen die in Absatz 1 genannten Richtlinien für das IKT-Projektmanagement vorsehen, dass das Leitungsorgan wie folgt über die Einleitung von IKT-Projekten, die sich auf kritische oder wichtige Funktionen des Finanzunternehmens auswirken, deren Fortschritte und die damit verbundenen Risiken unterrichtet wird:

a) einzeln oder zusammengefasst, je nach Bedeutung und Umfang der IKT-Projekte,

b) in regelmäßigen Abständen sowie erforderlichenfalls bei einzelnen Ereignissen.

Artikel 16

Beschaffung, Entwicklung und Wartung von IKT-Systemen

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen. Diese Richtlinien müssen

a) Sicherheitskonzepte und Methoden für die Beschaffung, Entwicklung und Wartung von IKT-Systemen enthalten,

b) verlangen, dass Folgendes angegeben wird:

   i) die technischen Spezifikationen und technischen IKT-Spezifikationen im Sinne von Artikel 2 Nummern 4 und 5 der Verordnung (EU) Nr. 1025/2012,

   ii) die Anforderungen für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen mit besonderem Schwerpunkt auf den Anforderungen an die IKT-Sicherheit und auf deren Genehmigung durch die betreffende Geschäftsfunktion und den IKT-Asset-Eigentümer gemäß den internen Governance-Regelungen des Finanzunternehmens;

c) Maßnahmen vorsehen, mit denen das Risiko einer unbeabsichtigten Veränderung oder einer vorsätzlichen Manipulation der IKT-Systeme während der Entwicklung, Wartung und Einführung dieser IKT-Systeme in der Produktionsumgebung gemindert wird.

(2) Die Finanzunternehmen entwickeln, dokumentieren und implementieren für die Tests und die Genehmigung aller IKT-Systeme vor ihrer Nutzung und nach ihrer Wartung gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii ein Verfahren für die Beschaffung, die Entwicklung und die Wartung von IKT-Systemen. Der Testumfang muss der Kritikalität der betreffenden Geschäftsprozesse und IKT-Assets angemessen sein. Die Tests müssen so ausgelegt sein, dass überprüft werden kann, ob neue IKT-Systeme ihrer geplanten Bestimmung angemessen sind, was auch die Qualität der intern entwickelten Software einschließt.

Zentrale Gegenparteien beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests neben den in Unterabsatz 1 genannten Anforderungen soweit relevant die folgenden Parteien ein:

a) Clearingmitglieder und Kunden,

b) interoperable zentrale Gegenparteien,

c) andere interessierte Parteien.

Zentralverwahrer beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests neben den in Unterabsatz 1 genannten Anforderungen soweit relevant die folgenden Parteien ein:

a) Nutzer,

b) kritische Versorgungsbetriebe und kritische Dienstleister,

c) andere Zentralverwahrer,

d) andere Marktinfrastrukturen,

e) alle sonstigen Institute, mit denen die Zentralverwahrer laut ihrer Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

(3) Im Rahmen des in Absatz 2 genannten Verfahrens sind Quellcodeprüfungen durchzuführen, die sowohl statische als auch dynamische Tests umfassen. Bei diesen Tests muss die Sicherheit internetexponierter Systeme und Anwendungen gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii getestet werden. Finanzunternehmen müssen

a) Schwachstellen und Anomalien im Quellcode ermitteln und analysieren,

b) einen Aktionsplan festlegen, um diese Schwachstellen und Anomalien zu beheben,

c) die Umsetzung dieses Aktionsplans überwachen.

(4) Im Rahmen des in Absatz 2 genannten Verfahrens muss spätestens zur Integrationsphase die Sicherheit von Softwarepaketen gemäß Artikel 8 Absatz 2 Buchstabe b Ziffern v, vi und vii getestet werden.

(5) Das in Absatz 2 genannte Verfahren muss Folgendes vorsehen:

a) in Nichtproduktionsumgebungen dürfen nur anonymisierte, pseudonymisierte oder randomisierte Produktionsdaten gespeichert werden,

b) Finanzunternehmen müssen die Integrität und Vertraulichkeit von Daten in Nichtproduktionsumgebungen schützen.

(6) Abweichend von Absatz 5 kann das in Absatz 2 genannte Verfahren vorsehen, dass Produktionsdaten nur für bestimmte Testanlässe, für begrenzte Zeiträume und nach Genehmigung durch die betreffende Funktion sowie nach Meldung solcher Anlässe an die IKT-Risikomanagement-Funktion gespeichert werden.

(7) Das in Absatz 2 genannte Verfahren muss Kontrollen zum Schutz der Integrität des Quellcodes von IKT-Systemen vorsehen, die intern oder von einem IKT-Drittdienstleister entwickelt und dem Finanzunternehmen von einem IKT-Drittdienstleister geliefert werden.

(8) Das in Absatz 2 genannte Verfahren muss vorsehen, dass proprietäre Software und nach Möglichkeit der Quellcode, der von IKT-Drittdienstleistern bereitgestellt wird oder aus Open-Source-Projekten stammt, vor ihrer Einführung in der Produktionsumgebung gemäß Absatz 3 analysiert und getestet werden.

(9) Die Absätze 1 bis 8 gelten auch für IKT-Systeme, die von nicht bei der IKT-Funktion angesiedelten Nutzern nach einem risikobasierten Ansatz entwickelt oder betrieben werden.

Artikel 17

IKT-Änderungsmanagement

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten sehen die Finanzunternehmen in den in Artikel 9 Absatz 4 Buchstabe e der Verordnung (EU) 2022/2554 genannten IKT-Änderungsmanagementverfahren für alle Änderungen an Software, Hardware, Firmware-Komponenten, Systemen oder Sicherheitsparametern alles Folgende vor:

a) eine Überprüfung, ob die IKT-Sicherheitsanforderungen erfüllt sind,

b) Mechanismen, die gewährleisten, dass die Funktionen, die Änderungen genehmigen, und die Funktionen, die für die Beantragung und Umsetzung dieser Änderungen zuständig sind, unabhängig sind,

c) eine klare Beschreibung der Aufgaben und Zuständigkeiten, um zu gewährleisten, dass

   i) Änderungen angegeben und geplant werden,

   ii) ein angemessener Übergang vorgesehen ist,

   iii) die Änderungen kontrolliert getestet und finalisiert werden,

   iv) eine wirksame Qualitätssicherung gewährleistet ist,

d) die Dokumentation und Kommunikation der Änderungen im Detail, wozu u. a. Folgendes zählt:

   i) Zweck und Umfang der Änderung,

   ii) Zeitplan für die Umsetzung der Änderung,

   iii) die erwarteten Ergebnisse;

e) die Angabe von Ausweichverfahren und -zuständigkeiten, einschließlich Verfahren und Zuständigkeiten für den Abbruch von Änderungen oder die Wiederherstellung, wenn Änderungen nicht erfolgreich implementiert wurden,

f) Verfahren, Protokolle und Tools für den Umgang mit Notfalländerungen, die angemessene Schutzvorkehrungen vorsehen,

g) Verfahren zur Dokumentation, Neubewertung, Bewertung und Genehmigung von Notfalländerungen, nachdem diese vorgenommen wurden, einschließlich Ausweichlösungen und Patches,

h) Angabe der potenziellen Auswirkungen einer Änderung auf bestehende IKT-Sicherheitsmaßnahmen und Bewertung, ob eine solche Änderung zusätzliche IKT-Sicherheitsmaßnahmen erfordert.

(2) Wenn zentrale Gegenparteien und Zentralverwahrer an ihren IKT-Systemen erhebliche Änderungen vorgenommen haben, unterziehen sie diese strengen Tests unter Simulation von Stressbedingungen.

Zentrale Gegenparteien beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests soweit relevant die folgenden Parteien ein:

a) Clearingmitglieder und Kunden,

b) interoperable zentrale Gegenparteien,

c) andere interessierte Parteien.

Zentralverwahrer beziehen in die Ausgestaltung und Durchführung der in Unterabsatz 1 genannten Tests soweit relevant die folgende Parteien ein:

a) Nutzer,

b) kritische Versorgungsbetriebe und kritische Dienstleister,

c) andere Zentralverwahrer,

d) andere Marktinfrastrukturen,

e) alle sonstigen Institute, mit denen die Zentralverwahrer laut ihrer IKT-Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

ABSCHNITT 8

Artikel 18

Physische Sicherheit und Sicherheit vor Umweltereignissen

(1) Im Rahmen der Schutzvorkehrungen zur Wahrung der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten verfassen, dokumentieren und implementieren die Finanzunternehmen Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen. Die Finanzunternehmen gestalten diese Richtlinien unter Berücksichtigung der Cyberbedrohungslage gemäß der nach Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 vorgenommenen Klassifizierung und unter Berücksichtigung des Gesamtrisikoprofils der IKT-Assets und der zugänglichen Informationsassets.

(2) Die in Absatz 1 genannten Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen müssen alles Folgende beinhalten:

a) einen Verweis auf den Abschnitt der Richtlinien, in dem es um die in Artikel 21 Absatz 1 Buchstabe g genannte Kontrolle der Zugangs- und Zugriffsrechte geht,

b) die Maßnahmen, mit denen die Räumlichkeiten und Rechenzentren des Finanzunternehmens und die vom Finanzunternehmen designierten sensiblen Bereiche, in denen IKT- und Informationsassets untergebracht sind, vor Angriffen, Unfällen und Umweltbedrohungen und -gefahren geschützt werden,

c) die Maßnahmen, mit denen die IKT-Assets inner- und außerhalb der Räumlichkeiten des Finanzunternehmens unter Berücksichtigung der Ergebnisse der IKT-Risikobewertung für diese IKT-Assets gesichert werden,

d) Maßnahmen, mit denen die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von IKT-Assets, Informationsassets und Einrichtungen für die physische Zugangskontrolle des Finanzunternehmens durch angemessene Wartung sichergestellt werden soll,

e) Maßnahmen, mit denen die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Daten gewahrt werden sollen, einschließlich

   i) der Vorgabe eines „leeren Schreibtischs“,

   ii) der Vorgabe eines „leeren Bildschirms“ bei Datenverarbeitungsanlagen.

Für die Zwecke des Buchstabens b müssen die Maßnahmen zum Schutz vor Umweltbedrohungen und -gefahren der Bedeutung der Räumlichkeiten, der Rechenzentren und der designierten sensiblen Bereiche und der Kritikalität der dort untergebrachten Geschäftstätigkeiten oder IKT-Systeme angemessen sein.

Für die Zwecke des Buchstabens c müssen die in Absatz 1 genannten Richtlinien für die physische Sicherheit und die Sicherheit vor Umweltereignissen angemessene Schutzmaßnahmen für unbeaufsichtigte IKT-Assets enthalten.

KAPITEL II

Richtlinien für Personalpolitik und Zugangskontrolle

Artikel 19

Richtlinien für Personalpolitik

Die Finanzunternehmen nehmen in ihre Richtlinien für Personalpolitik oder in ihre anderen einschlägigen Richtlinien alle nachstehend genannten IKT-sicherheitsbezogenen Elemente auf:

a) die Angabe und Zuweisung etwaiger spezifischer Zuständigkeiten im Bereich der IKT-Sicherheit,

b) die Vorgabe für die Mitarbeiter des Finanzunternehmens und des IKT-Drittdienstleisters, die IKT-Assets des Finanzunternehmens nutzen oder auf diese zugreifen,

   i) sich über die Richtlinien, Verfahren und Protokolle des Finanzunternehmens zur IKT-Sicherheit zu informieren und diese einzuhalten,

   ii) auf dem Laufenden darüber zu sein, welche Kanäle das Finanzunternehmen für die Meldung anomaler Verhaltensweisen geschaffen hat, wozu — soweit relevant — die gemäß der Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates ([11]) eingerichteten Meldekanäle zählen,

   iii) dem Finanzunternehmen nach Beendigung des Beschäftigungsverhältnisses alle in ihrem Besitz befindlichen IKT-Assets und materiellen Informationsassets, die Eigentum des Finanzunternehmens sind, auszuhändigen.

Artikel 20

Identitätsmanagement

(1) Um die Zuweisung der Nutzerzugriffsrechte gemäß Artikel 21 zu ermöglichen, entwickeln, dokumentieren und implementieren die Finanzunternehmen im Rahmen der Kontrolle der Zugangs- und Zugriffsrechte Richtlinien und Verfahren für das Identitätsmanagement, die die eindeutige Identifizierung und Authentifizierung der natürlichen Personen und Systeme, die auf Informationen der Finanzunternehmen zugreifen, gewährleisten.

(2) Die in Absatz 1 genannten Richtlinien für das Identitätsmanagement müssen alles Folgende vorsehen:

a) unbeschadet des Artikels 21 Absatz 1 Buchstabe c ist jedem Mitarbeiter des Finanzunternehmens oder Mitarbeitern der IKT-Drittdienstleister, die auf die Informationsassets und IKT-Assets des Finanzunternehmens zugreifen, eine eindeutige Identität zuzuweisen, die einem eindeutigen Nutzerkonto zugeordnet werden kann,

b) einen Lebenszyklusmanagementprozess für Identitäten und Konten, der die Erstellung, Änderung, Überprüfung und Aktualisierung, die vorübergehende Deaktivierung und die Beendigung aller Konten umfasst.

Für die Zwecke des Buchstabens a führen die Finanzunternehmen Aufzeichnungen über alle zugeordneten Identitäten. Diese Aufzeichnungen werden unbeschadet der im geltenden Unionsrecht und im nationalen Recht festgelegten Speicherpflichten nach einer Umstrukturierung des Finanzunternehmens oder nach Ablauf der Vertragsbeziehung aufbewahrt.

Für die Zwecke des Buchstabens b greifen die Finanzunternehmen beim Lebenszyklusmanagementprozess für Identitäten soweit möglich und angemessen auf automatisierte Lösungen zurück.

Artikel 21

Zugangskontrolle

Im Rahmen der Kontrolle der Zugangs- und Zugriffsrechte entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien, die alles Folgende vorsehen:

a) die Zuweisung der Rechte auf Zugang zu IKT-Assets nach dem Grundsatz „Kenntnis nur, wenn nötig“ („Need-to-know“), nach dem Grundsatz der Nutzungsnotwendigkeit („Need-to-use“) und nach dem Grundsatz der minimalen Berechtigung („Least privileges“), auch für den Fern- und Notfallzugang,

b) die Abtrennung der Aufgaben, einen ungerechtfertigten Zugang zu kritischen Daten zu verhindern oder die Zuweisung einer Kombination von Zugriffsrechten zu verhindern, die zur Umgehung von Kontrollen genutzt werden können,

c) eine Bestimmung zur Zurechenbarkeit, die die Nutzung generischer und gemeinsam genutzter Nutzerkonten so weit wie möglich einschränkt und die sicherstellt, dass die in den IKT-Systemen vorgenommenen Handlungen jederzeit einem Nutzer zugeordnet werden können,

([11]) Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. Oktober 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (ABl. L 305 vom 26.11.2019, S. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) eine Bestimmung zur Beschränkung des Zugangs zu IKT-Assets, die Kontrollen und Tools zur Verhinderung eines unbefugten Zugangs vorsieht,

e) Kontoverwaltungsverfahren für die Gewährung, Änderung oder Entziehung von Zugangsrechten für Nutzerkonten und generische Konten, insbesondere auch für generische Administratorkonten, die alles Folgende beinhalten:

   i) die Zuweisung der Aufgaben und Zuständigkeiten für die Gewährung, Überprüfung und Entziehung von Zugangsrechten,

   ii) die Zuweisung eines bevorrechtigten Zugangs, eines Notfallzugangs und eines Administratorzugangs nach dem Grundsatz der Nutzungsnotwendigkeit oder ad hoc bei allen IKT-Systemen,

   iii) den umgehenden Entzug der Zugangsrechte bei Beendigung des Beschäftigungsverhältnisses oder wenn der Zugang nicht länger erforderlich ist,

   iv) die Aktualisierung der Zugangsrechte, wenn Änderungen notwendig sind, mindestens aber einmal jährlich bei allen IKT-Systemen mit Ausnahme derjenigen, die kritische oder wichtige Funktionen unterstützen, und mindestens alle sechs Monate bei IKT-Systemen, die kritische oder wichtige Funktionen unterstützen;

f) Authentifizierungsmethoden, die alles Folgende vorsehen:

   i) die Nutzung von Authentifizierungsmethoden ist der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 vorgenommenen Klassifizierung und dem Gesamtrisikoprofil der IKT-Assets angemessen und trägt führenden Praktiken Rechnung,

   ii) die Nutzung starker Authentifizierungsmethoden entspricht den führenden Praktiken und Techniken für den Fernzugang zum Netz des Finanzunternehmens, für den bevorrechtigten Zugang, für den Zugang zu IKT-Assets, die kritische oder wichtige Funktionen unterstützen oder IKT-Assets, die öffentlich zugänglich sind,

g) physische Zugangskontrollen, die Folgendes einschließen:

   i) die Identifizierung und Protokollierung natürlicher Personen mit Zugangsberechtigung für Räumlichkeiten, Rechenzentren und die vom Finanzunternehmen designierten sensiblen Bereiche, in denen IKT- und Informationsassets untergebracht sind,

   ii) die Gewährung der Rechte auf physischen Zugang zu kritischen IKT-Assets nur für befugte Personen nach dem Grundsatz „Kenntnis nur, wenn nötig“ und dem Grundsatz der minimalen Berechtigung sowie ad hoc,

   iii) die Überwachung des physischen Zugangs zu Räumlichkeiten, Rechenzentren und die vom Finanzunternehmen designierten sensiblen Bereiche, in denen IKT- und/oder Informationsassets untergebracht sind,

   iv) die Überprüfung der physischen Zugangsrechte, um zu gewährleisten, dass unnötige Zugangsrechte umgehend entzogen werden.

Für die Zwecke von Buchstabe e Ziffer i legen die Finanzunternehmen die Speicherfrist fest und tragen dabei den Geschäftszielen und den Zielen für die Informationssicherheit, den Gründen für die Protokollierung des Ereignisses und den Ergebnissen der IKT-Risikobewertung Rechnung.

Für die Zwecke von Buchstabe e Ziffer ii verwenden die Finanzunternehmen für die Ausführung administrativer Aufgaben in IKT-Systemen nach Möglichkeit spezielle Konten. Für das Management des bevorrechtigten Zugangs greifen die Finanzunternehmen soweit möglich und angemessen auf automatisierte Lösungen zurück.

Für die Zwecke von Buchstabe g Ziffer i müssen die Identifizierung und Protokollierung der Bedeutung der Räumlichkeiten, der Rechenzentren und der designierten sensiblen Bereiche und der Kritikalität der dort untergebrachten Geschäftstätigkeiten oder IKT-Systeme angemessen sein.

Für die Zwecke von Buchstabe g Ziffer iii muss die Überwachung der gemäß Artikel 8 Absatz 1 der Verordnung (EU) 2022/2554 vorgenommenen Klassifizierung und der Kritikalität des Zugangsbereichs angemessen sein.

KAPITEL III

Erkennung IKT-bezogener Vorfälle und Reaktion

Artikel 22

Richtlinien für die Behandlung IKT-bezogener Vorfälle

Im Rahmen des Mechanismus zur Erkennung anomaler Aktivitäten, worunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle fallen, entwickeln, dokumentieren und implementieren die Finanzunternehmen Richtlinien für IKT-bezogene Vorfälle, in deren Rahmen sie

a) den in Artikel 17 der Verordnung (EU) 2022/2554 genannten Prozess für die Behandlung IKT-bezogener Vorfälle dokumentieren,

b) eine Liste der relevanten Kontakte erstellen, die mit internen Funktionen und externen Interessenträgern, die direkt an der IKT-Betriebssicherheit beteiligt sind, unter anderem in Bezug auf Folgendes unterhalten werden:

   i) die Erkennung und Überwachung von Cyberbedrohungen,

   ii) die Erkennung anomaler Aktivitäten,

   iii) das Schwachstellenmanagement;

c) technische, organisatorische und operative Mechanismen zur Unterstützung des Prozesses für die Behandlung IKT-bezogener Vorfälle einrichten, implementieren und betreiben, darunter auch Mechanismen, die eine rasche Erkennung anomaler Tätigkeiten und Verhaltensweisen gemäß Artikel 23 ermöglichen,

d) gemäß Artikel 15 der Delegierten Verordnung (EU) 2024/1772 ([12]) und gemäß allen nach Unionsrecht geltenden Speichervorschriften alle Nachweise im Zusammenhang mit IKT-bezogenen Vorfällen so lange aufbewahren, wie es für die Zwecke der Datenerhebung unbedingt erforderlich und der Kritikalität der betreffenden Unternehmensfunktionen, unterstützenden Prozesse sowie IKT- und Informationsassets angemessen ist,

e) Mechanismen zur Analyse bedeutender oder wiederkehrender IKT-bezogener Vorfälle und -Muster in Bezug auf Anzahl und Auftreten IKT-bezogener Vorfälle einrichten und implementieren.

Für die Zwecke des Buchstabens d bewahren die Finanzunternehmen die dort genannten Nachweise auf sichere Weise auf.

Artikel 23

Erkennung anormaler Aktivitäten und Kriterien für die Erkennung IKT-bezogener Vorfälle und die Reaktion auf solche Vorfälle

(1) Um IKT-bezogene Vorfälle und anormale Aktivitäten wirkungsvoll zu erkennen und wirkungsvoll darauf reagieren zu können. legen die Finanzunternehmen klare Aufgaben und Zuständigkeiten fest.

(2) Der in Artikel 10 Absatz 1 der Verordnung (EU) 2022/2554 genannte Mechanismus zur umgehenden Erkennung anomaler Aktivitäten, darunter auch Probleme bei der Leistung von IKT-Netzwerken und IKT-bezogene Vorfälle, muss es den Finanzunternehmen ermöglichen,

a) alles Folgende zu sammeln, zu überwachen und zu analysieren:

   i) interne und externe Faktoren, darunter zumindest die gemäß Artikel 12 gesammelten Protokolle, die Informationen von Unternehmens- und IKT-Funktionen sowie alle etwaigen, von Nutzern des Finanzunternehmens gemeldeten Probleme,

   ii) potenzielle interne und externe Cyberbedrohungen unter Berücksichtigung der üblicherweise von Angreifern verwendeten Szenarien und der auf Bedrohungsanalysen beruhenden Szenarien,

([12]) Delegierte Verordnung (EU) 2024/1772 der Kommission vom 13. März 2024 zur Ergänzung der Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Festlegung der Kriterien für die Klassifizierung von IKT-bezogenen Vorfällen und Cyberbedrohungen, der Wesentlichkeitsschwellen und der Einzelheiten von Meldungen schwerwiegender Vorfälle (ABl. L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

iii) Meldungen IKT-bezogener Vorfälle durch einen IKT-Drittdienstleister des Finanzunternehmens, die in den Systemen und Netzwerken des IKT-Drittdienstleisters entdeckt wurden und Auswirkungen auf das Finanzunternehmen haben könnten,

b) anomale Aktivitäten und Verhaltensweisen festzustellen und Tools einzusetzen, die zumindest für IKT- und Informationsassets, die kritische oder wichtige Funktionen unterstützen, Warnmeldungen generieren, die auf anomale Aktivitäten und Verhaltensweisen aufmerksam machen,

c) die unter Buchstabe b genannten Warnmeldungen zu priorisieren, damit die festgestellten IKT-bezogenen Vorfälle innerhalb der von den Finanzunternehmen festgelegten erwarteten Abwicklungszeit sowohl während als auch außerhalb der Arbeitszeiten gelöst werden können,

d) sämtliche relevanten Informationen über alle anomalen Aktivitäten und Verhaltensweisen automatisch oder manuell aufzuzeichnen, zu analysieren und auszuwerten.

Für die Zwecke des Buchstabens b beinhalten die dort genannten Tools auch solche, die nach vorab definierten Regeln automatische Warnmeldungen zur Feststellung von Anomalien generieren, die die Vollständigkeit und Integrität der Datenquellen oder gesammelten Protokolle beeinträchtigen.

(3) Die Finanzunternehmen schützen jede Aufzeichnung anomaler Aktivitäten vor Manipulation und unbefugtem Zugriff und zwar unabhängig davon, ob diese Daten gespeichert sind oder gerade übermittelt oder verwendet werden.

(4) Für jede festgestellte anomale Aktivität protokollieren die Finanzunternehmen alle relevanten Informationen, die

a) die Feststellung von Datum und Uhrzeit der anomalen Aktivität ermöglichen,

b) die Feststellung von Datum und Uhrzeit der Erkennung der anomalen Aktivität ermöglichen,

c) die Feststellung der Art der anomalen Aktivität ermöglichen.

(5) Wenn die Finanzunternehmen die in Artikel 10 Absatz 2 der Verordnung (EU) 2022/2554 genannten Erkennungs- und Reaktionsprozesse für IKT-bezogene Vorfälle auslösen, tragen sie dabei allen folgenden Kriterien Rechnung:

a) Hinweisen darauf, dass in einem IKT-System oder -Netzwerk möglicherweise eine böswillige Aktivität stattgefunden hat oder dieses IKT-System oder -Netzwerk korrumpiert sein könnte,

b) Datenverlusten, die im Hinblick auf die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten festgestellt wurden,

c) festgestellten schädlichen Auswirkungen auf die Transaktionen und Operationen des Finanzunternehmens,

d) der Nichtverfügbarkeit von IKT-Systemen und -Netzwerken.

(6) Für die Zwecke des Absatzes 5 tragen die Finanzunternehmen auch der Kritikalität der betroffenen Dienstleistung Rechnung.

KAPITEL IV

Management der IKT-Geschäftsfortführung

Artikel 24

Komponenten der IKT-Geschäftsfortführungsleitlinie

(1) Die Finanzunternehmen nehmen in die in Artikel 11 Absatz 1 der Verordnung (EU) 2022/2554 genannte IKT-Geschäftsfortführungsleitlinie Folgendes auf:

a) eine Beschreibung

i) der Ziele der IKT-Geschäftsfortführungsleitlinie, darunter auch der Wechselwirkungen zwischen der IKT- und der allgemeinen Geschäftsfortführung, unter Berücksichtigung der Ergebnisse der in Artikel 11 Absatz 5 der Verordnung (EU) 2022/2554 genannten Business-Impact-Analyse,

ii) des Umfangs der Geschäftsfortführungsvorkehrungen, -pläne, -verfahren und -mechanismen samt etwaiger Beschränkungen und Ausschlüsse,

iii) des von den Geschäftsfortführungsvorkehrungen, -plänen, -verfahren und -mechanismen abzudeckenden Zeitraums,

iv) der Kriterien für die Aktivierung und Deaktivierung von IKT-Geschäftsfortführungsplänen, IKT-Reaktions- und Wiederherstellungsplänen und Krisenkommunikationsplänen;

b) Bestimmungen zu:

i) Governance und Organisation zur Umsetzung der IKT-Geschäftsfortführungsleitlinie, einschließlich Aufgaben, Zuständigkeiten und Eskalationsverfahren, wobei zu gewährleisten ist, dass ausreichende Ressourcen zur Verfügung stehen,

ii) der Abstimmung zwischen den IKT-Geschäftsfortführungsplänen und den allgemeinen Geschäftsfortführungsplänen, was zumindest alles Folgende angeht:

1. die potenziellen Ausfallszenarien, einschließlich der in Artikel 26 Absatz 2 genannten Szenarien,

2. die Ziele für die Wiederherstellung des Geschäftsbetriebs, wobei festzulegen ist, dass das Finanzunternehmen den Betrieb seiner kritischen oder wichtigen Funktionen nach einer Störung entsprechend den Vorgaben für die Wiederherstellungszeit und den Wiederherstellungspunkt wiederherstellen können muss;

iii) der Entwicklung von IKT-Geschäftsfortführungsplänen für schwerwiegende Betriebsstörungen als Teil dieser Pläne und der Priorisierung der IKT-Geschäftsfortführungsmaßnahmen nach einem risikobasierten Ansatz,

iv) Entwicklung, Tests und Überprüfung der IKT-Reaktions- und Wiederherstellungspläne gemäß den Artikeln 25 und 26,

v) der Überprüfung der Wirksamkeit umgesetzter Geschäftsfortführungsvorkehrungen, -pläne, -verfahren und -mechanismen gemäß Artikel 26,

vi) der Abstimmung der IKT-Geschäftsfortführungsleitlinie mit:

1. der in Artikel 14 Absatz 2 der Verordnung (EU) 2022/2554 genannten Kommunikationsstrategie,

2. den in Artikel 11 Absatz 2 Buchstabe e der Verordnung (EU) 2022/2554 genannten Kommunikations- und Krisenmanagementmaßnahmen.

(2) Zentrale Gegenparteien stellen zusätzlich zu den Anforderungen in Absatz 1 sicher, dass ihre IKT-Geschäftsfortführungsleitlinie

a) für ihre kritischen Funktionen eine Wiederherstellungszeit von maximal 2 Stunden vorsieht,

b) externen Verbindungen und wechselseitigen Abhängigkeiten innerhalb der Finanzinfrastrukturen Rechnung trägt, darunter Handelsplätzen, die von der zentralen Gegenpartei gecleart werden, Wertpapierliefer- und -abrechnungssystemen sowie Zahlungssystemen und Kreditinstituten, die von der zentralen Gegenpartei oder einer verbundenen zentralen Gegenpartei genutzt werden;

c) Vorkehrungen im Hinblick darauf verlangt,

i) die Fortführung kritischer oder wichtiger Funktionen der zentralen Gegenpartei ausgehend von Katastrophenszenarien sicherzustellen,

ii) einen sekundären Verarbeitungsstandort zu unterhalten, der die Fortführung kritischer oder wichtiger Funktionen der zentralen Gegenpartei in gleicher Weise wie am Primärstandort gewährleisten kann,

iii) einen sekundären Geschäftsstandort zu unterhalten oder zur sofortigen Verfügung zu haben, damit die Mitarbeiter die Dienstleistung weiter erbringen können, wenn der Primärstandort nicht verfügbar ist,

iv) die Einrichtung zusätzlicher Verarbeitungsstandorte zu erwägen, insbesondere falls die unterschiedlichen Risikoprofile des primären und des sekundären Standorts keine hinreichende Gewähr dafür bieten, dass die Ziele der zentralen Gegenpartei hinsichtlich der Geschäftsfortführung in allen Szenarien erreicht werden können.

Für die Zwecke von Buchstabe a führen die zentralen Gegenparteien Tagesabschlussprozesse und Zahlungen unter allen Umständen fristgerecht durch.

Für die Zwecke von Buchstabe c Ziffer i müssen die dort genannten Vorkehrungen die Verfügbarkeit angemessener Humanressourcen, die Höchstdauer eines Ausfalls der kritischen Funktionen, den Failover zu einem sekundären Standort und die Wiederherstellung an diesem sekundären Standort regeln.

Für die Zwecke von Buchstabe c Ziffer ii muss der dort genannte sekundäre Verarbeitungsstandort ein anderes geografisches Risikoprofil aufweisen als der Primärstandort.

(3) Zentralverwahrer stellen zusätzlich zu den Anforderungen in Absatz 1 sicher, dass ihre IKT-Geschäftsfortführungsleitlinie

a) etwaigen Verbindungen und wechselseitigen Abhängigkeiten gegenüber Nutzern, kritischen Versorgungsbetrieben und kritischen Dienstleistern, anderen Zentralverwahrern und anderen Marktinfrastrukturen Rechnung trägt,

b) verlangt, dass die Vorkehrungen für die Geschäftsfortführung vorsehen, dass die Vorgabe für die Wiederherstellungszeit für ihre kritischen oder wichtigen Funktionen maximal zwei Stunden beträgt.

(4) Handelsplätze stellen zusätzlich zu den Anforderungen in Absatz 1 sicher, dass ihre IKT-Geschäftsfortführungsleitlinie gewährleistet, dass

a) der Handel nach einer Störung innerhalb von zwei Stunden oder einer geringfügig längeren Frist wieder aufgenommen werden kann,

b) der Datenverlust bei allen IT-Diensten des Handelsplatzes nach einer Störung nahezu null beträgt.

Artikel 25

Test des IKT-Geschäftsfortführungsplans

(1) Beim Test der IKT-Geschäftsfortführungspläne gemäß Artikel 11 Absatz 6 der Verordnung (EU) 2022/2554 berücksichtigen die Finanzunternehmen ihre Business-Impact-Analyse (BIA) und die in Artikel 3 Absatz 1 Buchstabe b der vorliegenden Verordnung genannte IKT-Risikobewertung.

(2) Durch den in Absatz 1 genannten Test ihrer IKT-Geschäftsfortführungspläne beurteilen die Finanzunternehmen, ob sie die Fortführung ihrer kritischen oder wichtigen Funktionen gewährleisten können. Diese Tests müssen

a) ausgehend von Testszenarien durchgeführt werden, bei denen potenzielle Störungen simuliert werden und die eine angemessene Zahl von schwerwiegenden, aber plausiblen Szenarien umfassen,

b) gegebenenfalls Tests der von IKT-Drittanbietern erbrachten IKT-Dienstleistungen umfassen,

c) bei den in Artikel 11 Absatz 6 Unterabsatz 2 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, Szenarien für Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und Systeme enthalten,

d) darauf ausgelegt sein, die Annahmen, auf denen die Geschäftsfortführungspläne beruhen, einschließlich der Governance-Regelungen und Krisenkommunikationspläne, infrage zu stellen,

e) Verfahren enthalten, mit denen überprüft wird, ob die Mitarbeiter der Finanzunternehmen, die IKT-Drittdienstleister, die IKT-Systeme und die IKT-Dienste angemessen auf die gemäß Artikel 26 Absatz 2 gebührend berücksichtigten Szenarien reagieren.

Für die Zwecke des Buchstabens a nehmen die Finanzunternehmen in ihre Tests stets die bei Ausarbeitung der Geschäftsfortführungspläne berücksichtigten Szenarien auf.

Für die Zwecke des Buchstabens b berücksichtigen die Finanzunternehmen in gebührendem Umfang gegebenenfalls Szenarien, in denen die Insolvenz oder der Ausfall der IKT-Drittdienstleister oder politische Risiken im Sitzland der IKT-Drittdienstleister unterstellt werden.

Für die Zwecke des Buchstabens c wird bei den Tests überprüft, ob zumindest kritische oder wichtige Funktionen für ausreichend lange Zeit angemessen aufrechterhalten werden können und ob der normale Betrieb wiederhergestellt werden kann.

(3) Zentrale Gegenparteien beziehen in die in Absatz 1 genannten Tests ihrer IKT-Geschäftsfortführungspläne neben den Anforderungen in Absatz 2 folgende Parteien ein:

a) Clearingmitglieder,

b) externe Dienstleister,

c) relevante Institute in der Finanzinfrastruktur, mit denen zentrale Gegenparteien laut ihrer Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

(4) Zentralverwahrer beziehen in die in Absatz 1 genannten Tests ihrer IKT-Geschäftsfortführungspläne neben den Anforderungen in Absatz 2 gegebenenfalls folgende Parteien ein:

a) die Nutzer der Zentralverwahrer,

b) kritische Versorgungsbetriebe und kritische Dienstleister,

c) andere Zentralverwahrer,

d) andere Marktinfrastrukturen,

e) alle sonstigen Institute, mit denen die Zentralverwahrer laut ihrer Geschäftsfortführungsleitlinie wechselseitige Abhängigkeiten verbinden.

(5) Die Finanzunternehmen dokumentieren die Ergebnisse der in Absatz 1 genannten Tests. Alle bei diesen Tests festgestellten Schwachstellen werden analysiert, angegangen und dem Leitungsorgan zur Kenntnis gebracht.

Artikel 26

IKT-Reaktions- und Wiederherstellungspläne

(1) Bei der Ausarbeitung der in Artikel 11 Absatz 3 der Verordnung (EU) 2022/2554 genannten IKT-Reaktions- und Wiederherstellungspläne berücksichtigen die Finanzunternehmen die Ergebnisse der Business-Impact-Analyse (BIA) des Finanzunternehmens. Diese IKT-Reaktions- und Wiederherstellungspläne müssen

a) die Bedingungen für die Aktivierung oder Deaktivierung der Pläne sowie etwaige für deren Aktivierung oder Deaktivierung geltenden Ausnahmen festlegen;

b) beschreiben, welche Maßnahmen zu ergreifen sind, um die Verfügbarkeit, Integrität, Kontinuität und Wiederherstellung zumindest der IKT-Systeme und -Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens sicherzustellen;

c) so konzipiert sein, dass sie den Zielen für die Wiederherstellung des Geschäftsbetriebs der Finanzunternehmen gerecht werden;

d) dokumentiert und den an der Ausführung der IKT-Reaktions- und Wiederherstellungspläne beteiligten Mitarbeitern zur Verfügung gestellt werden und im Notfall leicht zugänglich sein;

e) sowohl kurz- als auch langfristige Wiederherstellungsoptionen vorsehen, insbesondere auch die teilweise Systemwiederherstellung;

f) die Ziele der IKT-Reaktions- und Wiederherstellungspläne sowie die Bedingungen festlegen, unter denen die Durchführung dieser Pläne für erfolgreich erklärt werden kann.

Für die Zwecke von Buchstabe d legen die Finanzunternehmen die Aufgaben und Zuständigkeiten klar fest.

(2) In den in Absatz 1 genannten IKT-Reaktions- und Wiederherstellungsplänen werden relevante Szenarien genannt, insbesondere auch Szenarien mit schwerwiegenden Betriebsstörungen und erhöhter Wahrscheinlichkeit, dass Störungen auftreten. In diesen Plänen werden Szenarien ausgearbeitet, die sich auf aktuelle Informationen über Bedrohungen und auf die Lehren aus früheren Betriebsstörungen stützen. Von den Finanzunternehmen werden alle folgenden Szenarien gebührend berücksichtigt:

a) Cyberangriffe und Umstellungen von der primären IKT-Infrastruktur auf die redundanten Kapazitäten, Backups und redundanten Systeme;

b) Szenarien, in denen die Qualität der Bereitstellung einer kritischen oder wichtigen Funktion auf ein inakzeptables Niveau absinkt oder diese Funktion ganz ausfällt und in denen die potenziellen Auswirkungen der Insolvenz oder sonstiger Ausfälle eines relevanten IKT-Drittdienstleisters gebührend berücksichtigt werden;

c) teilweiser oder vollständiger Ausfall von Räumlichkeiten, insbesondere auch von Büro- und Geschäftsräumen, sowie von Rechenzentren;

d) erheblicher Ausfall von IKT-Assets oder der Kommunikationsinfrastruktur;

e) Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitern oder von Mitarbeitern, die für die Gewährleistung der Betriebskontinuität zuständig sind;

f) Auswirkungen von Ereignissen im Zusammenhang mit Klimawandel und Umweltzerstörung, Naturkatastrophen, Pandemien und physischen Angriffen, insbesondere auch durch Eindringen und Terroranschläge;

g) Angriffe durch Insider;

h) politische und soziale Instabilität, sofern relevant auch im Sitzland des IKT-Drittdienstleisters und am Standort der Datenspeicherung und -verarbeitung;

i) weitverbreitete Stromausfälle.

(3) Sind die primären Wiederherstellungsmaßnahmen möglicherweise wegen Kosten, Risiken, Logistik oder unvorhergesehener Umstände kurzfristig nicht durchführbar, so werden in den in Absatz 1 genannten IKT-Reaktions- und Wiederherstellungsplänen auch Alternativen erwogen.

(4) Im Rahmen der in Absatz 1 genannten IKT-Reaktions- und Wiederherstellungspläne werden von den Finanzunternehmen Kontinuitätsmaßnahmen geprüft und durchgeführt, um Ausfälle von IKT-Drittdienstleistern, die IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen des Finanzunternehmens bereitstellen, zu mindern.

KAPITEL V

Bericht über die Überprüfung des IKT-Risikomanagementrahmens

Artikel 27

Format und Inhalt des Berichts über die Überprüfung des IKT-Risikomanagementrahmens

(1) Die Finanzunternehmen legen den in Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554 genannten Bericht über die Überprüfung des IKT-Risikomanagementrahmens in einem durchsuchbaren elektronischen Format vor.

(2) Die Finanzunternehmen nehmen in den in Absatz 1 genannten Bericht alle folgenden Informationen auf:

a) einen einleitenden Abschnitt, der Folgendes enthält:

   i) eine eindeutige Angabe des Finanzunternehmens, das Gegenstand des Berichts ist, und, sofern relevant, eine Beschreibung seiner Gruppenstruktur;

   ii) eine Beschreibung des Kontexts des Berichts mit Blick auf Art, Umfang und Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte des Finanzunternehmens, seine Organisation, die ermittelten kritischen Funktionen, die Strategie, die wichtigsten laufenden Projekte oder Tätigkeiten, die Beziehungen und seine Abhängigkeit von internen und per Vertrag vergebenen IKT-Dienstleistungen und -Systemen oder die Auswirkungen, die ein Totalverlust oder eine schwerwiegende Verschlechterung derartiger Systeme hinsichtlich kritischer oder wichtiger Funktionen und der Markteffizienz hätte;

   iii) eine Zusammenfassung der wichtigsten Veränderungen des IKT-Risikomanagementrahmens seit dem letzten vorgelegten Bericht;

   iv) eine Kurzzusammenfassung des aktuellen und auf kurze Sicht bestehenden IKT-Risikoprofils, der Bedrohungslage, der erachteten Wirksamkeit seiner Kontrollen und der Sicherheitslage des Finanzunternehmens;

b) das Datum der Genehmigung des Berichts durch das Leitungsorgan des Finanzunternehmens;

c) eine Beschreibung des Grunds für die Überprüfung des IKT-Risikomanagementrahmens nach Artikel 6 Absatz 5 der Verordnung (EU) 2022/2554;

d) das Anfangs- und Enddatum des Überprüfungszeitraums;

e) eine Angabe der für die Überprüfung verantwortlichen Funktion;

f) eine Beschreibung der wichtigsten Veränderungen und Verbesserungen des IKT-Risikomanagementrahmens seit der letzten Überprüfung;

g) eine Zusammenfassung der Ergebnisse der Überprüfung und eine detaillierte Analyse und Bewertung der Schwere der Schwächen, Mängel und Lücken des IKT-Risikomanagementrahmens im Überprüfungszeitraum;

h) eine Beschreibung der Maßnahmen zur Behebung festgestellter Schwächen, Mängel und Lücken, die alles Folgende enthält:

   i) eine Zusammenfassung der Maßnahmen, die zur Behebung festgestellter Schwächen, Mängel und Lücken ergriffen wurden;

   ii) ein voraussichtliches Datum für die Durchführung der Maßnahmen und Daten für die interne Kontrolle der Durchführung, einschließlich Informationen über den Stand der Durchführung dieser Maßnahmen zum Zeitpunkt der Ausarbeitung des Berichts, gegebenenfalls mit einer Erläuterung, ob die Gefahr besteht, dass Fristen nicht eingehalten werden;

   iii) die zu verwendenden Tools und die Nennung der für die Durchführung der Maßnahmen verantwortlichen Funktion, wobei anzugeben ist, ob es sich um interne oder externe Tools/Instrumente und Funktionen handelt;

   iv) eine Beschreibung der Auswirkungen der im Rahmen der Maßnahmen geplanten Veränderungen auf die finanziellen, personellen und materiellen Ressourcen des Finanzunternehmens, insbesondere auch auf die für die Durchführung etwaiger Korrekturmaßnahmen vorgesehenen Ressourcen;

   v) gegebenenfalls Informationen über das Verfahren zur Unterrichtung der zuständigen Behörde;

   vi) falls die festgestellten Schwächen, Mängel oder Lücken nicht Gegenstand von Korrekturmaßnahmen sind, eine ausführliche Erläuterung der Kriterien, die zur Analyse der Auswirkungen dieser Schwächen, Mängel oder Lücken herangezogen wurden, um das damit verbundene IKT-Restrisiko zu bewerten, sowie der Kriterien für das Eingehen des damit verbundenen Restrisikos;

i) Informationen über geplante Weiterentwicklungen des IKT-Risikomanagementrahmens;

j) Schlussfolgerungen aus der Überprüfung des IKT-Risikomanagementrahmens;

k) Informationen über frühere Überprüfungen, insbesondere auch

   i) eine Liste aller bisherigen Überprüfungen;

   ii) gegebenenfalls den Stand der Umsetzung der im letzten Bericht genannten Korrekturmaßnahmen;

   iii) falls sich die in früheren Überprüfungen vorgeschlagenen Korrekturmaßnahmen als unwirksam erwiesen oder zu unerwarteten Herausforderungen geführt haben, eine Beschreibung der Möglichkeiten für eine Verbesserung dieser Korrekturmaßnahmen oder der unerwarteten Herausforderungen;

l) die zur Ausarbeitung des Berichts herangezogenen Informationsquellen, die insbesondere auch alles Folgende beinhalten müssen:

   i) bei den in Artikel 6 Absatz 6 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen, bei denen es sich nicht um Kleinstunternehmen handelt, die Ergebnisse der internen Revisionen;

   ii) die Ergebnisse der Compliance-Bewertungen;

   iii) die Ergebnisse der Tests der digitalen operationalen Resilienz und gegebenenfalls die Ergebnisse der erweiterten Tests von IKT-Tools, -Systemen und -Prozessen auf Basis bedrohungsorientierter Penetrationstests (TLPT — Threat-Led Penetration Testing);

   iv) externe Quellen.

Wurde die Überprüfung nach aufsichtsrechtlichen Anweisungen oder Feststellungen, die sich aus einschlägigen Tests der digitalen operationalen Resilienz oder Auditverfahren ergeben, eingeleitet, so muss der Bericht für die Zwecke des Buchstabens c ausdrückliche Verweise auf diese Anweisungen oder Feststellungen enthalten, die Aufschluss über den Grund für die Einleitung der Überprüfung geben. Wurde die Überprüfung nach IKT-bezogenen Vorfällen eingeleitet, so muss der Bericht eine Liste aller IKT-bezogenen Vorfälle mit einer Analyse der Ursachen dieser Vorfälle enthalten.

Für die Zwecke von Buchstabe f enthält die Beschreibung eine Analyse der Auswirkungen der Veränderungen auf die Strategie für die digitale operationale Resilienz des Finanzunternehmens, auf den internen IKT-Kontrollrahmen des Finanzunternehmens und auf die IKT-Risikomanagement-Governance des Finanzunternehmens.

TITEL III

VEREINFACHTER IKT-RISIKOMANAGEMENTRAHMEN FÜR DIE IN ARTIKEL 16 ABSATZ 1 DER VERORDNUNG (EU) 2022/2554 GENANNTEN FINANZUNTERNEHMEN

KAPITEL I

Vereinfachter IKT-Risikomanagementrahmen

Artikel 28

Governance und Organisation

(1) Die in Artikel 16 Absatz 1 der Verordnung (EU) 2022/2554 genannten Finanzunternehmen müssen über einen internen Governance- und Kontrollrahmen verfügen, der ein wirksames und umsichtiges Management von IKT-Risiken gewährleistet, um ein hohes Niveau an digitaler operationaler Resilienz zu erreichen.

(2) Die in Absatz 1 genannten Finanzunternehmen stellen im Zuge ihres vereinfachten IKT-Risikomanagementrahmens sicher, dass ihr Leitungsorgan

a) die Gesamtverantwortung dafür trägt, dass der vereinfachte IKT-Risikomanagementrahmen im Einklang mit der Risikobereitschaft des Finanzunternehmens die Verwirklichung der Geschäftsstrategie des Finanzunternehmens ermöglicht, und sicherstellt, dass IKT-Risiken in diesem Zusammenhang berücksichtigt werden;

b) für alle IKT-bezogenen Funktionen klare Aufgaben und Zuständigkeiten festlegt;

c) die Ziele für die Informationssicherheit und die IKT-Anforderungen festlegt;

d) Folgendes genehmigt, überwacht und regelmäßig überprüft:

   i) die in Artikel 30 Absatz 1 dieser Verordnung genannte Klassifizierung der Informations-Assets des Finanzunternehmens, die Liste der ermittelten Hauptrisiken sowie die Business-Impact-Analyse und die zugehörigen Richtlinien;

   ii) die in Artikel 16 Absatz 1 Buchstabe f der Verordnung (EU) 2022/2554 genannten Geschäftsfortführungspläne des Finanzunternehmens sowie Gegen- und Wiederherstellungsmaßnahmen;

e) die nötigen Budgetmittel zuweist und mindestens einmal jährlich überprüft, um den Anforderungen des Finanzunternehmens an die digitale operationale Resilienz in Bezug auf alle Arten von Ressourcen gerecht werden zu können, einschließlich einschlägiger Programme zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen operationalen Resilienz sowie Vermittlung von IKT-Kompetenzen für alle Mitarbeiter;

f) die in den Kapiteln I, II und III dieses Titels enthaltenen Richtlinien und Maßnahmen festlegt und umsetzt, um das IKT-Risiko, dem das Finanzunternehmen ausgesetzt ist, zu ermitteln, zu bewerten und zu managen;

g) die notwendigen Verfahren, IKT-Protokolle und Tools ermittelt und implementiert, um sämtliche Informations- und IKT-Assets zu schützen;

h) sicherstellt, dass die Mitarbeiter des Finanzunternehmens über ausreichende Kenntnisse und Fähigkeiten entsprechend den zu managenden IKT-Risiken verfügen und diesbezüglich stets auf dem neuesten Stand gehalten werden, um die IKT-Risiken und deren Auswirkungen auf die Geschäftstätigkeit des Finanzunternehmens verstehen und bewerten zu können;

i) die Modalitäten des Meldewesens festlegt, die insbesondere auch die Häufigkeit, die Form und den Inhalt der Meldungen an das Leitungsorgan über die Informationssicherheit und die digitale operationale Resilienz regeln.

(3) Die in Absatz 1 genannten Finanzunternehmen können die Überprüfung der Einhaltung der Anforderungen für das IKT-Risikomanagement im Einklang mit den sektorspezifischen Rechtsvorschriften der Union und der Mitgliedstaaten an gruppeninterne IKT-Unternehmen oder an IKT-Drittdienstleister auslagern. Im Falle einer solchen Auslagerung bleiben die Finanzunternehmen weiterhin uneingeschränkt für die Überprüfung der Einhaltung der IKT-Risikomanagementanforderungen verantwortlich.

(4) Die in Absatz 1 genannten Finanzunternehmen sorgen für eine angemessene Trennung und die Unabhängigkeit von Kontrollfunktionen und internen Revisionsfunktionen.